# 安全なリモートアクセス

～ Windows からの ssh 利用 ～

総合情報処理センター
池永　全志
ike@cc.nagasaki-u.ac.jp

## 1　なぜ telnet じゃいけないの？

ある計算機からネットワーク経由で他の計算機を利用する場合には，これまで “telnet” や “rlogin”, “rsh” といったプログラム (コマンド) が使われてきました．しかし，現在のようにインターネットが広く一般に利用されるようになり，悪意を持った利用者がどこに潜んでいるかわからないような状況では，telnet や rsh といったコマンドはあまりに無防備です．ではどのようなところが無防備なのでしょうか．以下に，よく言われる二つの問題を紹介します．

1. **ネットワーク上にデータがそのまま流れる**
   telnet や rsh を使った通信では，発生したデータはそのままの形[†1] で相手先まで送られます．つまり，相手先までのネットワークの途中で，誰かがその経路を流れるデータをじっと見ていたとすると，そこを流れる通信の内容は全てその誰かに見られてしまいます．見られて困るような内容の通信はしていないと言う人もいますが，通信内容はともかくとして，相手先の計算機にアクセスするために入力したパスワードもそのままの形で流れているのです．自分の入力したパスワードがそのままの形でインターネット上を流れていると考えると，ぞっとしますね[†2] ．
2. **UNIX レベルのユーザ認証**
   telnet や rsh を使って相手先の計算機にアクセスする場合，その人のアクセスを許可するかどうかのユーザ認証には通常の UNIX のログイン名とパスワードが使われますので，パスワードは 8 桁しかありません．また，自分でパスワード変更をするまで常に同じパスワードが使われるため，誰かにパスワードをのぞき見されてしまうと，そのパスワードを使用して簡単に計算機へアクセスされてしまいます．

## 2　安全な接続のために (ssh のススメ)

それでは，インターネット経由で安全に計算機を利用するにはどうすればよいのでしょうか．この解決策の一つが，ssh(Secure SHell) の利用です．ssh は rlogin や rsh などに代わるものとして作られており，強力な認証と通信路の暗号化によって先ほどの二つの問題に対処し，インターネット経由での安全な接続を可能にしています．また ssh は rlogin 等の代わりになるだけでなく，安全に X(X Window System) で接続できる機能や，任意の TCP 接続を安全に転送 (フォワーディング) する機能なども備えているほか，IP Spoofing(偽装) などの様々な種類の攻撃に対応できるようになっています．これら ssh の動作や暗号化の手法，どのような攻撃を防御するのかなど，ssh に関する様々な情報は FAQ としてまとめられており，日本語に訳されたものも Web で公開されています (文末の URL を参照)．

---

[†1] 分割されたりはしますが．

[†2] ぞっとしない人は，今日からでいいのでぞっとして下さい．

telnet や rlogin に代わって ssh を利用するには，アクセスされる側 (リモート側つまりネットワークの向こう側) の計算機で ssh のサーバプログラム[†3] が動いている必要があり，またアクセスする側 (ローカル側つまり自分の手元) の計算機では ssh のクライアントプログラムを使用する必要があります．総合情報処理センタがユーザに提供しているサーバ[†4] では ssh のサーバプログラムが動いています．また ssh のクライアントプログラムとして，UNIX 用のもの，Microsoft Windows 用のものについては良質なフリーソフトウェアが存在します．Macintosh 用については，現在は商用のソフトウェアを利用する方がよいようです．

以降では，Microsoft Windows95 または 98(以降では単に Windows と表記) のパソコンから ssh サーバの動作している計算機に，ネットワーク経由で接続するために必要な設定について解説します．

## 3 Windows からの ssh の利用

Windows で動作するフリーの ssh のクライアントソフトウェアには何種類かのものがあるようですが，ここでは “ttssh” を紹介します．この ttssh は，Windows から UNIX の計算機に telnet する場合に使用するソフトウェアである “TeraTerm”(テラターム) [†5] に対して，ssh の機能を付加するものです．TeraTerm は画面の制御や日本語 (漢字コード) の取扱いなど，基本的な機能が非常にしっかりして安定しており，これをそのまま ssh 対応とするためのソフトウェアである ttssh との組合せは現在最もおすすめできるものです．

### 3.1 TeraTerm のインストール

まず，まだ TeraTerm を利用されてない方のために，TeraTerm のインストール方法を紹介します．既に TeraTerm Pro Ver.2.3 以上を利用されている方は，ここは飛ばしてかまいません．ttssh では，TeraTerm Pro Ver.2.3 以上が必要ですので，古い版の TeraTerm を使われている方はこの機会に入れ直してみて下さい．

TeraTerm Pro Ver.2.3 はインストーラが付属しているので，次のような手順で比較的簡単にインストールできます．

1. Web や ftp などでパッケージを取ってくる．
   1999 年 3 月 15 日現在の最新版は Ver.2.3 なので，“`ttermp23.zip`” を取ってくる．
   `http://hp.vector.co.jp/authors/VA002416/teraterm.html`
2. “`ttermp23.zip`” を適当なフォルダに展開する．
   (例) `D:\tmp` に展開
3. 展開したファイルの中の “`setup.exe`” を実行する．
   (例) `D:\tmp\setup.exe` を実行
   (a) 言語モードを選択して [Continue] を押す．
   (例) “Japanese” を選択．
   (b) 古い版の TeraTerm を実行中でないことの確認をしてくるので，もし実行していたら終了して，実行していなければそのままで [Continue] を押す．
   (c) キーボードの選択をして [Continue] を押す．
   (例) “IBM PC/AT (DOS/V) キーボード” を選択．

---

[†3] UNIX では sshd というプログラムが使われます．

[†4] いわゆる net，net2 サーバもそのうちのひとつです．

[†5] TeraTerm は telnet だけでなくシリアルポートを利用するターミナルソフトとしても使用でき，非常に便利です．

(d) TeraTermをインストールするフォルダ名を指定する.

(例) "C:\Program Files\Ttermpro" を指定.

4. 必要なファイルが指定したフォルダにコピーされ，インストール終了.

ttermpro.exe が TeraTermの本体となる.

インストールが完了したら，最低限必要な設定をするためにTeraTermを起動します(先ほどのインストール例ではC:\Program Files\Ttermpro\ttermpro.exeを起動). 起動すると，"New connection" のウィンドウが開いてtelnetでどこかへ接続しようとするので(図1参照)，まずは Cancel ボタンを押してこのウィンドウを閉じます.

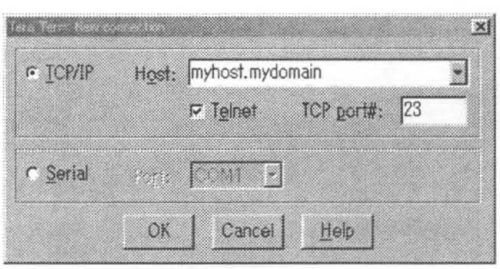


図 1: New connection ウィンドウ

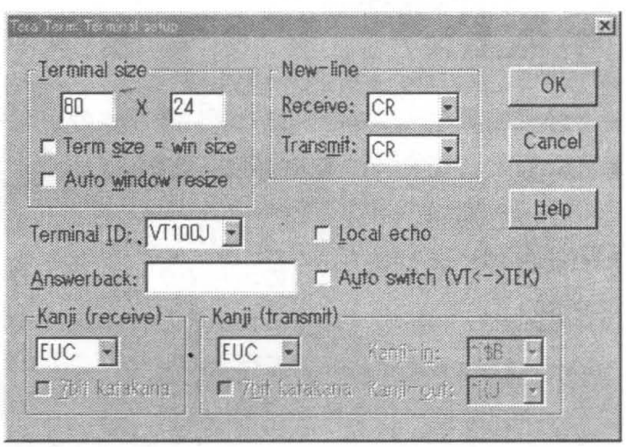


図 2: Terminal setup ウィンドウ

続いて，以下の内容に従って設定を行います.

- TeraTermウィンドウのメニューから，[ Setup ] → [ Terminal ] と選択するとSetupウィンドウが開く(図2参照).
- 真ん中付近の「Terminal ID:」を "VT100J" に設定する.
- 下側の「Kanji(receive)」と「Kanji(transmit)」を両方とも "EUC" に設定する.
- OK ボタンを押す.
- TeraTermウィンドウのメニューから，[ Setup ] → [ Save setup ] を選択し設定を保存する.
  その際，TeraTerm本体と同じフォルダ内に "teraterm.ini" というファイル名で保存すれば，次回以降の起動時に自動的に読み込まれる.
  (先ほどの例では C:\Program Files\Ttermpro\teraterm.ini)

### 3.2 ttsshのインストール

続いて，次のような手順でttsshのインストールを行います.

1. Webやftpなどでパッケージを取ってくる.
   1999年3月15日現在の最新版は Ver.1.4なので，"ttssh14.zip" を取ってくる.
   http://www.zip.com.au/~roca/ttssh.html
2. "ttssh14.zip" を TeraTermをインストールしたフォルダに展開する.
   (例) C:\Program Files\Ttermpro\に展開.
3. "ttssh.exe" が本体となる. 以後は "ttermpro.exe" ではなく "ttssh.exe" を使用する.

### 3.3 公開鍵，秘密鍵の作成

ttssh のインストールが終ったら，次に認証に使用する公開鍵及び秘密鍵を作成します．認証のための文字列 (パスフレーズ) を鍵生成の段階で盗まれたのでは元も子もありませんので，鍵の作成は必ず手元の計算機のコンソールから行うようにします．ttssh には鍵を生成するためのコマンドが含まれていないため，別途これを入手する必要があります．次のような手順でインストールして下さい．

1. *Web* や *ftp* などでパッケージを取ってくる．
   `ftp://ftp.cs.hut.fi/pub/ssh/contrib/ssh-1.2.14-win32bin.zip`
2. “`ssh-1.2.14-win32bin.zip` ” を展開する．
   (例) `C:\ssh\` など

続いて，インストールした一連のプログラムの中から，“`ssh-keygen`” コマンドを使用して次のような手順で秘密鍵と公開鍵を生成します．

1. MS-DOS プロンプトを起動する (DOS 窓を開く)．
2. 秘密鍵などを保存するためのホームディレクトリを set コマンドで指定する．
   (例) `C:\home` をホームディレクトリに指定．
3. “`ssh-keygen`” コマンドを実行する．
   (例) `C:\ssh\ssh-keygen -C host`
4. 生成した秘密鍵 (`identity` というファイル) をどこに置くかを聞いてくるので入力する．
   (例) `C:\home\.ssh\identity`
5. パスフレーズを入力する．
   パスフレーズが通常の UNIX パスワード (8 文字) より短くては意味が無いので，自分で覚えやすくて比較的難しく，ある程度長い文字列を使うようにする．
6. 同じパスフレーズを再度入力する．
7. 秘密鍵が “`identity`” という名前で，公開鍵が “`identity.pub`” という名前で生成される．
   (例) `C:\home\.ssh\identity` , `C:\home\.ssh\identity.pub`

```
C:\> set HOME=C:\home ↵
C:\> C:\ssh\ssh-keygen -C host ↵
Initializing random number generator...
Generating p: ........++ (distance 152)
Generating q: ................++ (distance 186)
Computing the keys...
Testing the keys...
Key generation complete.
Enter file in which to save the key (C:\home\.ssh\identity): ↵
Enter passphrase: ************ ↵←←← パスフレーズを入力
Enter the same passphrase again: ************ ↵←←← (もう一度)
Your identification has been saved in C:\home\.ssh\identity.
Your public key is:
1024 37 167642112956358317735619099844934153525980 17…(略)…3739 host
Your public key has been saved in C:\home\.ssh\identity.pub
```

生成した秘密鍵はそのまま手元のパソコンで使用しますが，公開鍵は，接続先の (ssh サーバが動作している) 計算機に入れておく必要があります．公開鍵は他人に見られてもかまわないものなので，ftp 等の暗号化されていない経路経由で転送してかまいません．先ほどの例を使って具体的に説明すると，鍵を生成した手元のパソコンの中にある`C:\home\.ssh\identity.pub` という公開鍵ファイルを接続先の計算機に転送し，`/home/taro/.ssh/authorized_keys` というファイル名で保存しておきます．この公開鍵ファイルはアスキーファイルなので，ftp を使用して転送する場合には，アスキーモードで転送するようにして下さい．また，ftp を使用する際に入力するパスワードは既存の telnet 同様，無防備な状態ですから，これらの操作は少なくとも学内の計算機間に限るなど (比較的) 安全なネットワーク上で行うようにするか，もしくは ftp した後，すぐに ssh で接続してパスワード変更をするなど，パスワードの漏洩に注意する必要があります．

### 3.4 ttssh の設定

公開鍵と秘密鍵の設定が終わったら，ttssh を起動し，ssh 関連の設定を行います．(先ほどのインストール例では`C:\Program Files\Ttermpro\ttssh.exe` を起動)．起動すると，“New connection” のウィンドウが開いて telnet でどこかへ接続しようとするので，TeraTerm のときと同様に，まず Cancel ボタンを押してこのウィンドウを閉じ，続いて以下の内容に従って設定を行います (図 3 参照)．

- ttssh ウィンドウのメニューから，[ Setup ] → [ SSH Authentication ] と選択する．
- 「User Name」のところに，接続先の計算機でのログイン名を入力する．
- 「Use RSA key to login」にチェックをする．
- その横の「Private key file」のところに，秘密鍵 (identity ファイル) の場所を入力する．
  (例) `C:\home\.ssh\identity`
- OK ボタンを押す．
- ttssh ウィンドウのメニューから，[ Setup ] → [ Save setup ] を選択し設定を保存する．
  先ほどと同様，TeraTerm(ttssh) 本体と同じフォルダ内に “`teraterm.ini`” というファイル名で保存すれば，次回以降の起動時に自動的に読み込まれる．
  (例) `C:\Program Files\Ttermpro\teraterm.ini`

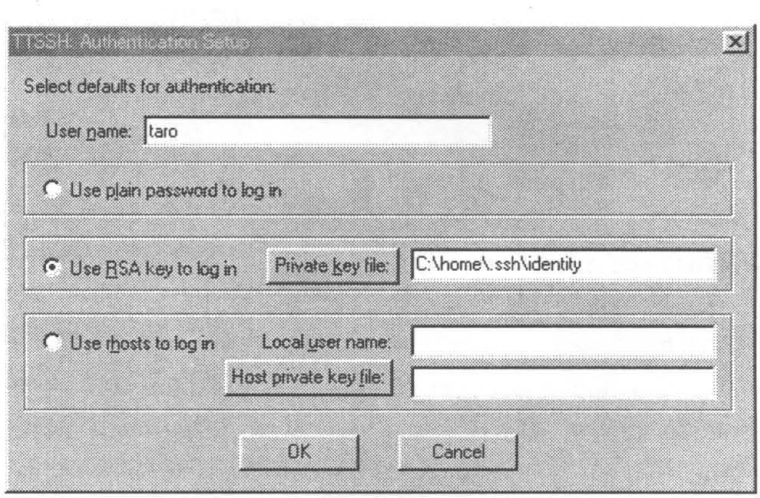


図 3: SSH Authentication 設定ウィンドウ

### 3.5 接続

これで全ての設定が終わりました．“**ttssh.exe**” コマンドを起動すると，図 4 のような新規接続ウィンドウが開くので必要な情報を入力し，さらに図 5 のウィンドウが開いたらパスフレーズを入力することにより ssh での接続が可能となります．

1. 「Host:」に (ssh サーバの動作している) 接続先のホスト名を書く．
2. 「Service」の部分は “SSH” を選択してチェックする．
3. 「TCP port#:」の部分が “22” になっていることを確認し，OK ボタンを押す．
4. 認証ウィンドウが開いたら「User name:」,「Passphrase:」を入力し，OK ボタンを押す．

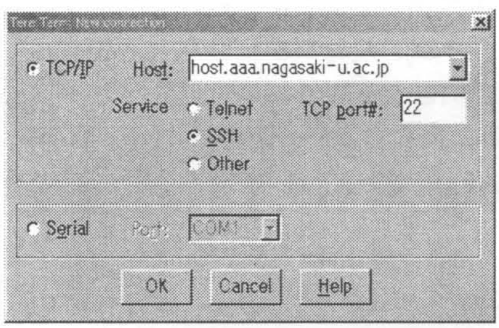


図 4: ttssh による新規接続ウィンドウ

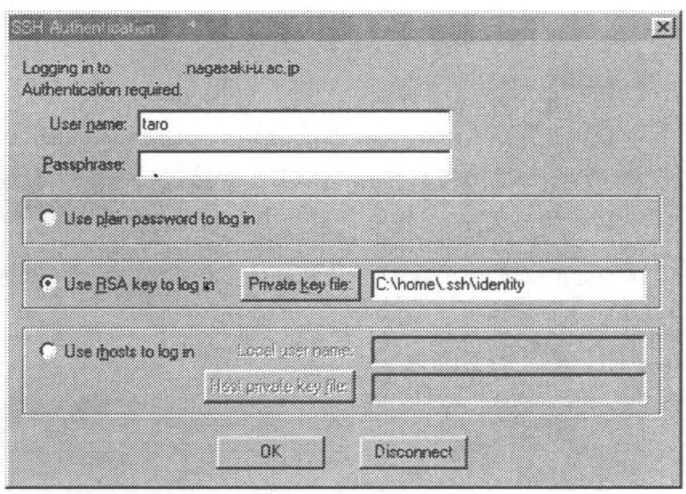


図 5: ssh 接続を行う場合の認証ウィンドウ

## 4 URL's

- ssh の本家 = **http://www.ssh.fi/**
- ttssh の本家 = **http://www.zip.com.au/~roca/ttssh.html**
- TeraTerm のページ
  **http://hp.vector.co.jp/authors/VA002416/teraterm.html**
- コマンドラインベースの ssh ソフト群
  **ftp://ftp.cs.hut.fi/pub/ssh/contrib/**
- フリーの ssh2 クライアント
  **http://www.net.lut.ac.uk/psst/**
- Macintosh 用の ssh クライアントソフトウェア (F-Secure)
  **http://www.datafellows.fi/f-secure/fclintp.htm**
  **http://www.europe.datafellows.com/japan/f-secure/product.html**
- ssh 関連情報のリンク集
  **http://www.vacia.is.tohoku.ac.jp/~s-yamane/FAQ/ssh/link.html**
- itojun さんの ssh についてのチュートリアルスライド
  **http://www.itojun.org/paper/wide-9811-ssh-tutorial/**
- One Time Password と SSH のススメ
  **http://fukuda.aist-nara.ac.jp/~yasuhi-a/linux/ssh/lj.html**